

AD-A244 576



4 NBD

1

December 1991

MTR₁₀₉₉₃

Jonathan T. Trostle

The Serial Product of
Controlled Signalling
Systems



Approved for public release;
distribution unlimited.

92-01506



MITRE

Bedford, Massachusetts

92 1 16 092

December 1991

MTR₁₀₉₉₃

Jonathan T. Trostle

The Serial Product of
Controlled Signalling
Systems



Accession For	
NTIS	CR/CI
DTIC	ISD
Unannounced	
Justification	
By	
Distribution/	
Availability	
Dist	Availability
A-1	

CONTRACT SPONSOR NCSC
CONTRACT NO. DAAB07-91-C-N751
PROJECT NO. 8350
DEPT. G117

Approved for public release;
distribution unlimited.

MITRE


The MITRE Corporation
Bedford, Massachusetts

Department Approval: Mark E. Nadel
Mark E. Nadel
Department Head

MITRE Project Approval: Dale M. Johnson
Dale M. Johnson
Project Leader, 8350

ABSTRACT

The controlled signalling system is a finite-state deterministic model of information disclosure on a computer system. The model includes high-level and low-level cooperating processes. The processes cooperate to covertly send data from the high-level process (transmitter) to the low-level process (receiver). The capacity of a controlled signalling system is a measure of the amount of information the high-level process can disclose to the low-level process. The serial product is a binary operation on the class of controlled signalling systems. The capacity of the serial product of two controlled signalling systems can be strictly greater than the capacities of the individual systems. The r -controlled signalling systems are a subclass of controlled signalling systems; for r -controlled signalling systems, the serial product capacity is the maximum of the individual capacities.



ACKNOWLEDGMENTS

This work was supported by the National Security Agency under Contract F19628-89-C-0001 and completed under MITRE Project 8350. I wish to thank Todd Wittbold for the many helpful discussions concerning controlled signalling systems and the material in this paper. I would also like to thank both Dale Johnson for some useful advice on \LaTeX and Jon Millen for some helpful comments.

TABLE OF CONTENTS

SECTION	PAGE
1 Introduction	1
2 Controlled Signalling Systems	3
3 Serial Products and An Example	14
4 r-Controlled Signalling Systems	24
List of References	33
Distribution List	35

SECTION 1

INTRODUCTION

This paper is concerned with products of controlled signalling systems; a controlled signalling system is a deterministic finite-automata model with two players, or processes. This model was developed by Wittbold in [5]. The programs cooperate in order to covertly send data from one process, the transmitter, to the other process, the receiver. Controlled signalling systems illustrate the potential for application of graph-theoretic and information-theoretic techniques to modelling problems in computer security. Since the work in this paper is concerned with products of controlled signalling systems, we will briefly review controlled signalling systems and some of the main results of [5]. Further details are given in Section 2.

The controlled signalling system is a finite-state deterministic model with a high-level process acting as transmitter and a low-level process acting as receiver. The transmitter and receiver alternate turns; a turn consists of an input into the finite-state automata and an output delivered to the input source (transmitter or receiver.) The transmitter is able to send information to the receiver, since its turns affect the state of the system, and, hence, the receiver's output is affected by the transmitter's inputs. The receiver is not allowed to directly view the transmitter's inputs and outputs. The goal of the spies who have installed the programs is to maximize the rate of information flow from the transmitter to the receiver. In a controlled signalling system, the receiver chooses a sampling strategy (a policy); under a fixed strategy, the receiver's next input is a function of the receiver's preceding inputs and outputs. Each fixed strategy gives rise to a discrete noiseless channel, ([4]); the capacity of the controlled signalling system is defined as the supremum of the capacities of the induced discrete noiseless channels. The problem of choosing the optimal policy is solved in [5].

The coding theorem of [5] (Theorem 2.1) shows that block-policy codes with rates arbitrarily close to the capacity of the system exist; these codes are explicit algorithms for communication between transmitter and receiver. It is also proved that no block-policy codes with rates exceeding the capacity can exist. A key result (Theorem 2.2) of [5] is the optimality equation:

$$V^{n+1}(s) = \max_r \sum_t \mu(r; s, t) V^n(t),$$

where $V^n(s)$ is the maximum, over all strategies, of the number of length n output words that can be produced under a fixed strategy starting with a signal of type s , and $\mu(r, s, t)$ is the control array for the controlled signalling system. This equation allows one to compute optimal strategies and associate a piecewise linear operator Φ with the

controlled signalling system. For positive control arrays, the capacity of the controlled signalling system is the log of the largest eigenvalue of this associated operator.

In this paper, we study products of controlled signalling systems. The product of two controlled signalling systems \mathcal{S}_1 and \mathcal{S}_2 is obtained by taking unions of the transmitter and receiver alphabets and taking the Cartesian product of the sets of states. A state transition resulting from an input in \mathcal{S}_1 is accomplished by allowing the \mathcal{S}_1 component of the state to change as it would in \mathcal{S}_1 while the \mathcal{S}_2 component of the state remains unchanged. The output delivered to the inputting process is the same as would be delivered in \mathcal{S}_1 given the same input and \mathcal{S}_1 component of the state. The analogous statement holds for inputs in \mathcal{S}_2 . An intuitively plausible formula is

$$cap(\mathcal{S}_1 \times \mathcal{S}_2) = \max\{cap(\mathcal{S}_1), cap(\mathcal{S}_2)\} \quad (1)$$

where $cap(\mathcal{S})$ is the capacity of a controlled signalling system \mathcal{S} . We give an example in section 3 to show that (1) does not hold for controlled signalling systems. In section 4, we investigate a subclass of controlled signalling systems, the class of r -controlled signalling systems. For r -controlled signalling systems, the transmitter edges have a transitive closure property. In this case, we derive a new control array and prove equation (1).

SECTION 2

CONTROLLED SIGNALLING SYSTEMS

This section is devoted to a careful review of the key results on controlled signalling systems from [5]. The controlled signalling system is a finite-state deterministic model of information transfer from one process in a computer system, the transmitter, to another process, the receiver. Each process has an input alphabet and an output alphabet; the processes alternate turns. A turn consists of a process input, a change of state determined by the input and current state, and an output similarly determined and delivered to the inputting process. A process has no knowledge of the other process's outputs. We interpret the evolution of the turns as a game in which both processes cooperate to maximize information flow to the receiver. We now give a precise definition.

Definition 2.1 (Controlled Signalling System) A controlled signalling system is a 7-tuple $\langle S, I_T, I_R, O, next, out, a_0 \rangle$ where

1. S is a finite nonempty set of states.
2. I_R and I_T are finite disjoint nonempty sets of input symbols for the receiver and transmitter, respectively. $I = I_R \cup I_T$.
3. O is a finite nonempty set of output symbols.
4. $next : S \times I \rightarrow S$ is a function determining the next state from the current state and current input.
5. $out : S \times I \rightarrow O$ determines the current output from the current state and current input.
6. $a_0 \in S$ is the initial state.

We will sometimes write si in place of $next(s, i)$ where $s \in S$ and $i \in I$.

In [5], the following question is tackled: if the receiver is going to submit inputs based on a fixed strategy (a strategy is a function from the receiver's previous sequence of inputs and outputs into the set of inputs), how can the receiver choose a strategy which maximizes information flow from the transmitter to the receiver? Given the definition of receiver strategies, a natural definition of the capacity of controlled signalling systems was given in [5]. In order to make this paper self-contained, we now give these definitions.

Definition 2.2 (Receiver Strategy) A receiver strategy, or policy, is a sequence of functions

$$\pi = \pi_1, \pi_2, \dots,$$

such that for each $n \geq 1$,

$$\pi_n : (I_R \times O)^{n-1} \rightarrow I_R.$$

Intuitively, we think of the receiver submitting inputs i_1, \dots, i_{n-1} on turns t_1, \dots, t_{n-1} and receiving outputs o_1, \dots, o_{n-1} , where turn t_1 is the initial turn of the system. The receiver input for turn t_n under strategy π is

$$\pi_n(i_1 o_1, i_2 o_2, \dots, i_{n-1} o_{n-1}).$$

A controlled signalling system with fixed receiver strategy π maps naturally to a discrete noiseless channel. In [5], the capacity of a controlled signalling system is defined to be the supremum of the capacities of the associated discrete noiseless channels.

Definition 2.3 (Discrete Noiseless Channel) A discrete noiseless channel is a triple $C = (I, O, \vdash)$, where

1. I is a finite set of input symbols.
2. O is a finite set of output symbols.
3. $\vdash : I^* \rightarrow O^*$ is a function mapping strings of input symbols to strings of output symbols such that:

(a) $\vdash : I^n \rightarrow O^n$.

(b) If

$$x = x_1, \dots, x_m$$

and

$$y = x_1, \dots, x_m, y_{m+1}, \dots, y_{m+k}$$

are strings of input symbols where $k \geq 1$, we say that y is an extension string of x ; we denote this fact by $x \leq y$. If $x \leq y$, then $\vdash(x) \leq \vdash(y)$.

We now reproduce the definition of capacity for a discrete noiseless channel:

Definition 2.4 If A is a finite set, we let $|A|$ denote the cardinality of the set A . All logarithms will be to the base 2. If $C = (I, O, \vdash)$ is a discrete noiseless channel, we define

$$\text{cap}(C) = \limsup_{n \rightarrow \infty} \frac{\log(|\vdash(I^n)|)}{n}.$$

We now give the map which associates a fixed receiver strategy for a controlled signalling system S with a discrete noiseless channel.

Proposition 2.1 ([5]) Let S be a controlled signalling system and $a \in S$ a state of S . Let

$$\pi = \pi_1, \pi_2, \dots$$

be a receiver strategy. Then for each $n \geq 1$ and each $h_1, \dots, h_n \in I_T^n$, there are unique sequences $s_0, \dots, s_n \in S^{n+1}$ and $i_1 o_1 \dots i_n o_n \in (I_R \times O)^n$ such that the following system of equations is satisfied:

1. $s_0 = a$,
2. $s_t = s_{t-1} h_t i_t \quad 1 \leq t \leq n$,
3. $i_t = \pi_t(i_1 o_1 \dots i_{t-1} o_{t-1}) \quad 1 \leq t \leq n$, and
4. $o_t = \text{out}(s_{t-1} h_t, i_t) \quad 1 \leq t \leq n$.

In the above proposition, we say that $(i_1 o_1 \dots i_n o_n)$ satisfies the system equations for π with initial condition a and transmitter input string $h_1 h_2 \dots h_n$. The following proposition is an immediate consequence of Proposition 2.1.

Proposition 2.2 1. The map $\vdash_{(\pi, a)}: I_T^n \rightarrow (I_R \times O)^n$, defined by the condition

$$\vdash_{(\pi, a)}(h_1 \dots h_n) = (i_1 o_1 \dots i_n o_n)$$

if and only if $(i_1 o_1 \dots i_n o_n)$ satisfies the system equations for π with initial condition a and transmitter input string $h_1 h_2 \dots h_n$, is well-defined.

2. $c_{(\pi, a)} = (I_T, I_R \times O, \vdash_{(\pi, a)})$ is a discrete noiseless channel.

We can now define the capacity of a controlled signalling system.

Definition 2.5 Let a_0 be the initial state of the controlled signalling system S . We define

$$Ch(S) = \{c_{(\pi, a_0)} : \pi \text{ a receiver strategy}\}.$$

The capacity of S is

$$cap(S) = \sup_{c \in Ch(S)} cap(c).$$

$Ch(S)$ is the space of covert channels associated with the controlled signalling system S .

We will shortly define block-policy codes which are a natural extension of block codes. Given the definition of receiver strategy and block-policy codes, Wittbold ([5]) proves a coding theorem which shows that the definition of capacity is satisfactory. The coding theorem states that there are no block-policy codes with rates greater than the capacity but that there exist codes with rates as close to the capacity as desired. We now define some additional notation.

Definition 2.6 We denote the set of all receiver strategies by Π . A receiver strategy, or policy, of length n is a sequence of functions

$$\pi = \pi_1, \pi_2, \dots, \pi_n$$

such that for each k , $n \geq k \geq 1$,

$$\pi_k : (I_R \times O)^{k-1} \rightarrow I_R.$$

We let Π_n denote the set of receiver strategies of length n .

Definition 2.7 If $\{x_n\}$ is an infinite sequence, we define

$$rate\{x_n\} = \limsup_{n \rightarrow \infty} \frac{\log x_n}{n}. \quad (2)$$

If f is a function and the set X is contained in the domain of f , we define $f(X) = \{f(x) : x \in X\}$. Let S be a controlled signalling system, $a \in S$ a state, and π a strategy of length m , where $m \geq n$. Proposition 2.1 holds if we fix n and replace the receiver strategy with a receiver strategy of length m , $m \geq n$. In this situation, we say that $(i_1 o_1 \dots i_n o_n)$ satisfies the system equations for π with initial condition a and transmitter input string $h_1 h_2 \dots h_n$. Thus the map $\vdash_{(\pi, a)} : I_T^n \rightarrow (I_R \times O)^n$, defined by the condition

$$\vdash_{(\pi, a)} (h_1 \dots h_n) = (i_1 o_1 \dots i_n o_n)$$

if and only if $(i_1 o_1 \dots i_n o_n)$ satisfies the system equations for π with initial condition a and transmitter input string $h_1 h_2 \dots h_n$, is well-defined. We now define

$$D^n(\mathcal{S}, \pi, a) = \vdash_{(\pi, a)} (I_T^n).$$

We also define

$$d^n(\mathcal{S}, a) = \max_{\pi \in \Pi_n} |D^n(\mathcal{S}, \pi, a)|,$$

$$d(\mathcal{S}, a) = \text{rate}\{d^n(\mathcal{S}, a)\},$$

and

$$D^n(\mathcal{S}, \pi) = D^n(\mathcal{S}, \pi, a_0).$$

We will drop the \mathcal{S} from these expressions when the controlled signalling system is obvious from the context.

Proposition 2.1 shows that, given a receiver strategy π of length at least n and state a , there is for each string of n transmitter input symbols, $h_1 h_2 \dots h_n$, a unique state sequence $s_0 s_1 \dots s_n$. We define

$$\text{endpt}(\pi, a; h_1 h_2 \dots h_n) = s_n.$$

If there exist $h_1, h_2, \dots, h_m \in I_T$ and $i_1, i_2, \dots, i_m \in I_R$ such that $b = a_0 h_1 i_1 h_2 i_2 \dots h_m i_m$, we say that b is a reachable state.

We are now ready to give the definition of block-policy codes.

Definition 2.8 A block-policy code is a 5-tuple

$$B = (b, k_0, n_0, X, \pi)$$

where n_0, k_0 are integers. Also,

1. $b \in S$ is a reachable state, the basepoint of the code.
2. $\pi \in \Pi_{n_0}$ is a length n_0 strategy.
3. $X \subseteq I_T^{n_0}$ is a collection of codewords satisfying
 - (a) $|X| = 2^{k_0}$,
 - (b) $\vdash_{(\pi, b)}$ is 1:1 on X ,
 - (c) If $h_1 h_2 \dots h_{n_0} \in X$, then $\text{endpt}(\pi, b; h_1 h_2 \dots h_{n_0}) = b$.

The rate of the code is k_0/n_0 .

Condition (b) ensures the receiver will know what transmitter word was sent from inspection of its own i-o word. Condition (c) ensures that the system will return to state b every n_0 combined transmitter receiver turns; thus repeated concatenation of the finite strategy π with itself gives an infinite strategy that transfers data at the rate of k_0 bits every n_0 turns.

We can now state the coding theorem of [5].

Theorem 2.1 Let S be a controlled signalling system with $\text{cap}(S) = c > 0$. We then have

1. There are no block-policy codes with rates greater than c .
2. For each $\epsilon > 0$, there is a block-policy code with rate greater than $c - \epsilon$.
3. $c = d(a_0)$.

The proof of this theorem is in [5](pp.98-100).

We now develop the necessary framework to present the optimality equation (Theorem 2.2). The optimality equation will yield a dynamic programming approach to computing optimal receiver strategies; in combination with Theorem 2.3 (Bellman [1]), it yields an iterative algorithm for computing the capacity of a controlled signalling system. The optimality equation is an inductive formula for counting receiver input-output strings under optimal receiver strategies; the key to this approach is the definition of types. The types definition yields an equivalence relation on receiver input-output strings; if two strings are equivalent, they have the same "growth properties." Also, there are only a finite number of equivalence classes. We will now make these remarks more precise.

Definition 2.9 For each n , we define

$$\text{Sig}^n(a_0) = \bigcup_{\pi \in \Pi_n} D^n(\pi, a_0).$$

Let $\beta = i_1 o_1 \dots i_n o_n \in (I_R \times O)^n$, and let $h_1 h_2 \dots h_n \in I_T^n$. $h_1 h_2 \dots h_n$ is consistent with β if and only if there exists $s_0 s_1 \dots s_n \in S^n$ such that

1. $s_0 = a_0$,

2. $s_t = s_{t-1}h_t i_t$ $1 \leq t \leq n$, and
3. $o_t = \text{out}(s_{t-1}h_t, i_t)$ $1 \leq t \leq n$.

Definition 2.10 (Types) Let $\beta = i_1 o_1 \dots i_n o_n \in \text{Sig}^n(a_0)$. β is called a receiver output string of length n . $\text{type}(\beta) = \{a \in S : \text{there exists } h_1 h_2 \dots h_n \in I_T^n \text{ such that } h_1 h_2 \dots h_n \text{ is consistent with } \beta \text{ and } a_0 h_1 i_1 \dots h_n i_n = a\}$.

The equivalence relation on receiver output strings discussed in the remarks above defines receiver output strings β_1 and β_2 to be equivalent if $\text{type}(\beta_1) = \text{type}(\beta_2)$. The next proposition ensures that we can count receiver output strings by type; receiver output strings with the same type have the same extension strings, and these extension strings have the same type.

Let $A \subseteq S$ and $i \in I_R$. We define

$$\mathcal{O}(A, i) = \{o \in O : \text{there exists } a \in A, h \in I_T, \text{ such that } \text{out}(ah, i) = o\}.$$

Proposition 2.3 (Growth Properties) Let β_1, β_2 be receiver output strings of length n where $\text{type}(\beta_1) = \text{type}(\beta_2)$. For any $i \in I_R$ and $o \in O$, we have

1. $\beta_1 i o \in \text{Sig}^{n+1}(a_0)$ if and only if $o \in \mathcal{O}(\text{type}(\beta_1), i)$.
2. If $o \in \mathcal{O}(\text{type}(\beta_1), i)$, then

$$\begin{aligned} \text{type}(\beta_1 i o) = \{s \in S : \text{there exist } v \in \text{type}(\beta_1), h \in I_T, \\ \text{such that } v h i = s \text{ and } \text{out}(v h, i) = o\}. \end{aligned}$$

3. If $o \in \mathcal{O}(\text{type}(\beta_1), i)$, then $\text{type}(\beta_1 i o) = \text{type}(\beta_2 i o)$.

We are now ready to define the control array of a controlled signalling system. We will obtain a piecewise linear operator $\Phi : R^n \rightarrow R^n$ such that the capacity of the controlled signalling system is equal to $\log \lambda$ where λ is the largest positive eigenvalue of Φ .

Definition 2.11 (Control Array) Let \mathcal{S} be a controlled signalling system, and let τ_1, \dots, τ_l be an enumeration of the types of \mathcal{S} . Let i_1, \dots, i_R be an enumeration of the receiver input alphabet. We define the following array of integers to be the control array of \mathcal{S} :

$$\mu(r, s, t) = |\{o : \beta i_r o \in \text{Sig}^{n+1}(a_0), \beta \text{ has length } n, \text{type}(\beta) = s, \text{ and } \text{type}(\beta i_r o) = t\}|.$$

Proposition 2.3 shows that the control array is well-defined. We will now define the *Ext* functions which will lead us to the optimality equation (Theorem 2.2).

Definition 2.12 Let $Q \subseteq \text{Sig}^m(a_0)$, and let $\pi_{m+1} : (I_R \times O)^m \rightarrow I_R$. We define

$$\text{Ext}^1(Q; \pi_{m+1}) = \{\beta \pi_{m+1}(\beta) o : \beta \in Q \text{ and } o \in O(\text{type}(\beta), \pi_{m+1}(\beta))\}.$$

Let $\pi_{m+1}, \dots, \pi_{m+n}$ be functions such that $\pi_{m+k} : (I_R \times O)^{m+k-1} \rightarrow I_R$, $1 \leq k \leq n$. For $n \geq 2$ we define

$$\begin{aligned} \text{Ext}^n(Q; \pi_{m+1} \dots \pi_{m+n}) = \\ \text{Ext}^1(\text{Ext}^{n-1}(Q; \pi_{m+1} \dots \pi_{m+n-1}); \pi_{m+n}). \end{aligned}$$

We now give a lemma that will be helpful in the proof of Theorem 2.2.

Lemma 2.1 Let Q_1 and Q_2 be disjoint subsets of $\text{Sig}^m(a_0)$. Let $\pi^1 = \pi_{m+1}^1 \dots \pi_{m+n}^1$, $\pi^2 = \pi_{m+1}^2 \dots \pi_{m+n}^2$, and $\pi = \pi_{m+1} \dots \pi_{m+n}$ be sequences of functions such that

$$\pi, \pi_{m+k}^1, \pi_{m+k}^2 : (I_R \times O)^{m+k-1} \rightarrow I_R \quad 1 \leq k \leq n.$$

Suppose $\pi_{m+k}(q) = \pi_{m+k}^i(q)$ if $q \in Q_i \times (I_R \times O)^{k-1}$, $1 \leq k \leq n$, $i = 1, 2$. We then have

$$\text{Ext}^n(Q_1 \cup Q_2; \pi) = \text{Ext}^n(Q_1; \pi^1) \cup \text{Ext}^n(Q_2; \pi^2).$$

We now define the V^n functions.

Definition 2.13 We define

$$\Pi_{m,n} = \{\pi : \pi = \pi_{m+1} \dots \pi_{m+n} \text{ where } \pi_{m+k} : (I_R \times O)^{m+k-1} \rightarrow I_R, 1 \leq k \leq n\}.$$

For $Q \subseteq \text{Sig}^m(a_0)$ and $n \geq 1$, we define

$$V^n(Q) = \max_{\pi \in \Pi_{m,n}} |\text{Ext}^n(Q, \pi)|.$$

We also define $V^0(Q) = 1$. When we want to make the dependence of V^n on the controlled signalling system \mathcal{S} explicit, we will write $V^n(\mathcal{S}, Q)$ in place of $V^n(Q)$. If $Q = \{\beta\}$, we write $V^n(\beta)$ in place of $V^n(Q)$. We define $\pi \in \Pi_{m,n}$ to be n -optimal for Q if and only if $|\text{Ext}^n(Q; \pi)| = V^n(Q)$.

We are now ready to present the optimality equation.

Theorem 2.2 1. Let $Q \subseteq \text{Sig}^m(a_0)$, and let $\pi \in \Pi_{m,n}$. π is n -optimal for Q if and only if for each $\beta \in Q$, π is n -optimal for β . It follows that

$$V^n(Q) = \sum_{\beta \in Q} V^n(\beta).$$

2. Let $\beta \in \text{Sig}^m(a_0)$. For all $n \geq 0$,

$$V^{n+1}(\beta) = \max_{i \in I_R} \left\{ \sum_{o \in O(\text{type}(\beta), i)} V^n(\beta i o) \right\}.$$

3. Let S be a controlled signalling system, and let $\{\tau_1, \dots, \tau_l\}$ be the set of types for S . Let β_1 and β_2 be elements in $\text{Sig}^m(a_0)$. If $\text{type}(\beta_1) = \text{type}(\beta_2)$, then

$$V^n(\beta_1) = V^n(\beta_2).$$

Thus V^n is well-defined on the set of types for $n \geq 0$, and

$$V^{n+1}(s) = \max_{1 \leq r \leq R} \left\{ \sum_{1 \leq t \leq l} \mu(r; s, t) V^n(t) \right\}$$

where $I_R = \{i_1 \dots i_R\}$.

This theorem is proved in [5].

By Theorem 2.1, an algorithm to compute the integers $d^n(a_0) = \max_{\pi \in \Pi_n} |D^n(\pi, a_0)|$ will yield the capacity of the controlled signalling system S . If we let $\tau_1 = \{a_0\} = \text{type}(\epsilon)$, where ϵ is the empty string and we use the fact that

$$D^n(\pi, a_0) = \text{Ext}^n(\epsilon, \pi_1 \dots \pi_n),$$

we obtain $d^n(a_0) = V^n(1)$.

We now define the piecewise linear operator $\Phi : R^l \rightarrow R^l$ by defining the s th coordinate of Φ :

$$\Phi_s(x) = \max_{1 \leq r \leq R} \left\{ \sum_{1 \leq t \leq l} \mu(r; s, t) x_t \right\}.$$

The optimality equation may be expressed as

$$V^{n+1} = \Phi(V^n).$$

$V^n(1)$ is the first coordinate of

$$d^n = \Phi^n(d^0), \quad (3)$$

where d^0 is the vector of all 1's. We define $d(s) = \text{rate}\{d^n(s)\}$ where s is the s th coordinate in (3.) In [5], a partial order on coordinate indices is defined: $s_0 \rightsquigarrow s_n$ if

$$\mu(r_1; s_0, s_1)\mu(r_2; s_1, s_2) \dots \mu(r_n; s_{n-1}, s_n) > 0$$

for some choice of indices $r_1, s_1, \dots, r_n, s_{n-1}$. The control array μ is connected if the equivalence relation obtained by defining indices s and t to be equivalent, if $s \rightsquigarrow t$ and $t \rightsquigarrow s$, has only one component. In [5], Wittbold shows that $d(s) = d(t)$ for all indices s and t if the control array is connected. The equivalence class containing an index s is denoted by $[s]$. We define the operator $\tilde{\Phi} : R^l \rightarrow R^l$ by defining the s th coordinate of $\tilde{\Phi}$:

$$\tilde{\Phi}_s(x) = \max_{1 \leq r \leq R} \left\{ \sum_{t \in [s]} \mu(r; s, t) x_t \right\},$$

if $1 \leq s \leq l$. Let \tilde{d}^0 be the vector with l components all equal to 1. We define $\tilde{d}^n = \tilde{\Phi}^n(\tilde{d}^0)$. We denote the s th coordinate of \tilde{d}^n by $\tilde{d}^n(s)$. We also define

$$\tilde{d}(s) = \text{rate}\{\tilde{d}^n(s)\};$$

we then have the following proposition from [5].

Proposition 2.4 *Let μ be a control array, and let s be a coordinate index. We have*

$$d(s) = \max_{\{s_0: s_0 \rightsquigarrow s\}} \tilde{d}(s_0).$$

Thus the problem of computing the capacity of a controlled signalling system is reduced to computing the capacity of a controlled signalling system with a connected control array. The control array μ is positive if all the elements $\mu(r; s, t)$ are positive; clearly any positive control array is connected. In this case, the common value is denoted by $d(\mu)$. It is also shown in [5] that any connected control array μ can be approximated by a positive control array; there exists a positive control array μ_p such that $d(\mu_p)$ is as close to $d(\mu)$ as desired. We now state this result:

Proposition 2.5 *Let μ be a connected control array. For $\epsilon > 0$, we define*

$$\mu^\epsilon(r; s, t) = \begin{cases} \mu(r; s, t) & \text{if } \mu(r; s, t) > 0 \\ \epsilon & \text{if } \mu(r; s, t) = 0. \end{cases}$$

There exists a constant $K > 0$ such that for all $\epsilon > 0$,

$$d(\mu) \leq d(\mu^\epsilon) \leq d(\mu) + \log(1 + K\epsilon).$$

We will now give a definition in order to present the theorem of Bellman [1].

Definition 2.14 We let

$$\Delta^{T-1} = \{(x_1, x_2, \dots, x_T) : \sum_s x_s = 1, x_s \geq 0, 1 \leq s \leq T\}.$$

We also define $\phi : \Delta^{T-1} \rightarrow \Delta^{T-1}$ by

$$\phi^n(P) = \frac{\Phi^n(P)}{\bar{1} \cdot \Phi(P)}$$

where $\bar{1}$ denotes the vector of all 1's, and \cdot denotes the standard inner product.

We can now present the theorem which gives the capacity of a controlled signalling system with positive control array μ as the log of the largest positive eigenvalue of μ .

Theorem 2.3 (Bellman [1]) Let μ be a positive control array, and let Φ and ϕ be the associated operators. Then

1. Φ has a unique eigenvector $e \in \Delta^{T-1}$. Let $\Phi(e) = \lambda e$.
2. $\lambda > 0$ and e is positive.
3. For any $P \in \Delta^{T-1}$ we have $\lim_{n \rightarrow \infty} \phi^n(P) = e$.
4. $d(\mu) = \log(\lambda)$.

SECTION 3

SERIAL PRODUCTS AND AN EXAMPLE

We will now define the serial product of two controlled signalling systems.

Definition 3.1 (Serial Product) The serial product of two controlled signalling systems

$$S_1 = \langle S_1, I_{1T}, I_{1R}, O_1, next_1, out_1, a_{10} \rangle$$

and

$$S_2 = \langle S_2, I_{2T}, I_{2R}, O_2, next_2, out_2, a_{20} \rangle$$

is the controlled signalling system

$$S_1 \times S_2 = \langle S_1 \times S_2, I_{1T} \cup I_{2T}, I_{1R} \cup I_{2R}, O_1 \cup O_2, next_{12}, out_{12}, (a_{10}, a_{20}) \rangle$$

where:

1. $S_1 \times S_2$ is the Cartesian product of the sets S_1 and S_2 .
2. We assume $I_{1R} \cap I_{2R} = \emptyset$ and $I_{1T} \cap I_{2T} = \emptyset$.
3. We define $I_1 = I_{1R} \cup I_{1T}$, $I_2 = I_{2R} \cup I_{2T}$, and

$$next_{12}((s_1, s_2), i) = \begin{cases} (next_1(s_1, i), s_2) & \text{if } i \in I_1 \\ (s_1, next_2(s_2, i)) & \text{if } i \in I_2. \end{cases}$$

4. We define

$$out_{12}((s_1, s_2), i) = \begin{cases} out_1(s_1, i) & \text{if } i \in I_1 \\ out_2(s_2, i) & \text{if } i \in I_2. \end{cases}$$

Let π_1 be a strategy for the controlled signalling system S_1 . It is trivial to extend π_1 to a strategy π for $S_1 \times S_2$, such that π agrees with π_1 on elements of $(I_{1R} \times O)^n$ for all $n \geq 0$. Thus a block-policy code B_1 for S_1 can be extended to a block-policy code B for $S_1 \times S_2$ by replacing state b with state (b, a_0) , extending π_1 as above to a strategy π on S , and otherwise leaving B unchanged. The code B has the same rate as B_1 . Hence by Theorem 2.1, we must have

$$cap(S_1 \times S_2) \geq \max\{cap(S_1), cap(S_2)\}.$$

A natural question at this point is whether the following formula holds:

$$\text{cap}(\mathcal{S}_1 \times \mathcal{S}_2) = \max\{\text{cap}(\mathcal{S}_1), \text{cap}(\mathcal{S}_2)\}. \quad (4)$$

We say the controlled signalling system \mathcal{S} has the transmitter (receiver) self-loop property if there exists $i \in I_T$ ($i \in I_R$) such that $si = s$ for all states $s \in S$. It is easy to find examples of controlled signalling systems \mathcal{S}_1 and \mathcal{S}_2 without both transmitter and receiver self-loop properties such that (4) does not hold.

The following example will show that (4) does not hold for controlled signalling systems even in the case where both \mathcal{S}_1 and \mathcal{S}_2 have transmitter and receiver self-loop properties. The next section of the paper will be devoted to finding restrictions on controlled signalling systems that will allow us to prove a formula similar to (4.)

We let

$$\mathcal{S}_1 = \langle S_1, I_{1T}, I_{1R}, O_1, \text{next}_1, \text{out}_1, a_{10} \rangle$$

where $S_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $I_{1T} = \{v, w, x, y, z\}$, $I_{1R} = \{a, b\}$, and $O_1 = \{1, 2\}$ (see figure 1). For $i \in I_R$,

$$\text{next}_1(s, i) = \begin{cases} 8 & \text{if } s = 6, i = b \\ 7 & \text{if } s = 5, i = b \\ 5 & \text{if } s \in \{1, 2\}, i = b \\ 6 & \text{if } s \in \{3, 4\}, i = b \\ s & \text{otherwise.} \end{cases}$$

For $i \in I_T$, the *next* function is described by the unlabeled edges in figure 1. An edge directed from state s in the figure to state t defines $\text{next}(s, i) = t$ for at least one $i \in I_T$. Since there are at most 5 unlabeled edges leaving any state and $|I_T| = 5$, this definition is satisfactory. For $i \in I_R$, we have

$$\text{out}_1(s, i) = \begin{cases} 2 & \text{if } s = 2, i = b \\ 2 & \text{if } s = 4, i = b \\ 2 & \text{if } s = 6, i = b \\ 1 & \text{otherwise.} \end{cases}$$

For $i \in I_T$, and $s \in S$, we define $\text{out}_1(s, i) = 1$. Also, $a_{10} = 0$.

The transmitter outputs of a controlled signalling system play no role in the arguments of this paper or in [5]. In figure 1, an edge with label i/o directed from state s to state t gives that $\text{next}_1(s, i) = t$ and $\text{out}_1(s, i) = o$. As mentioned above, unlabeled edges correspond to transmitter inputs into the *next* function. We let $\overline{\mathcal{S}}_1$ be an isomorphic copy of \mathcal{S}_1 .

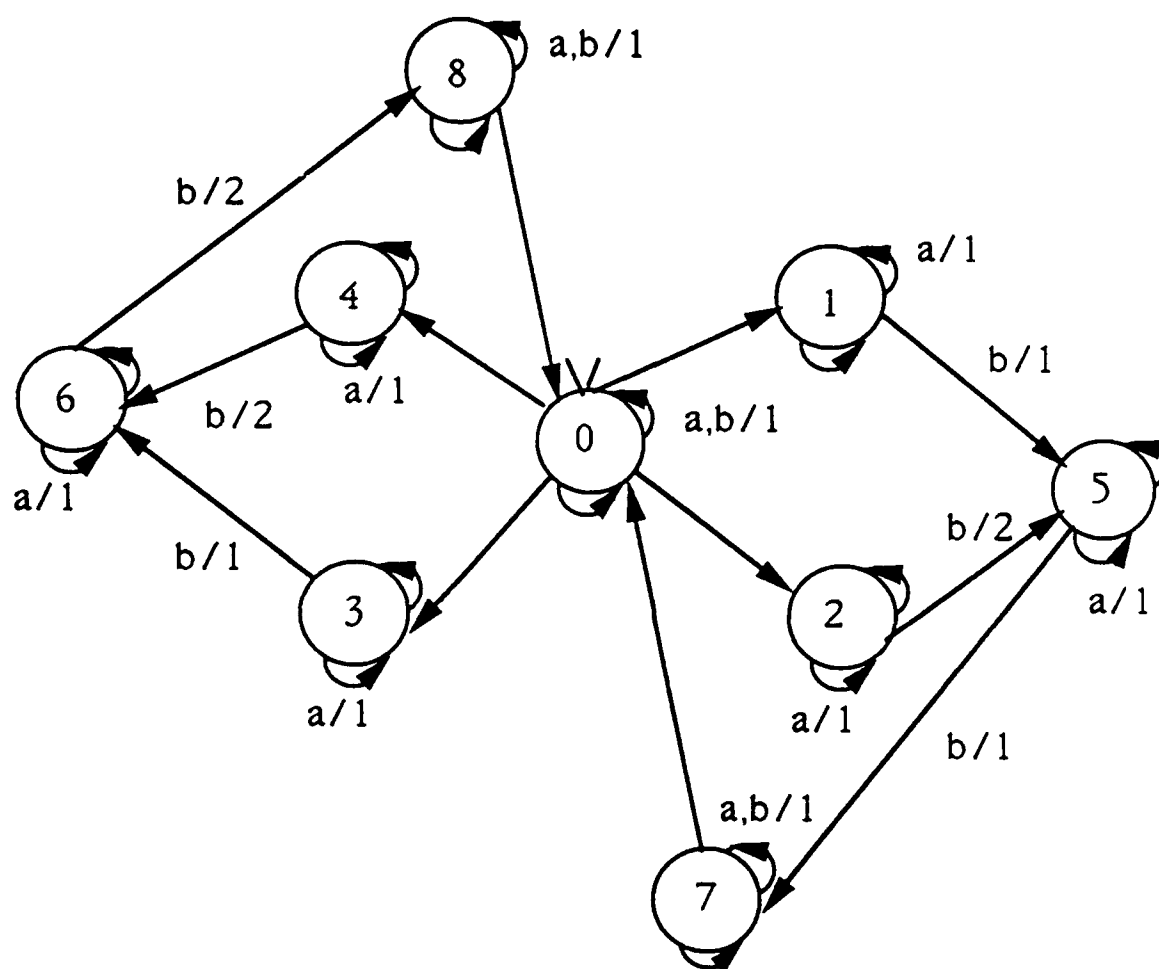


Figure 1: \mathcal{S}_1

We will now prove that

$$\text{cap}(\mathcal{S}_1 \times \overline{\mathcal{S}_1}) > \text{cap}(\mathcal{S}_1), \quad (5)$$

thus showing that (4) does not hold for controlled signalling systems.

Before giving this proof, we will give an intuitive explanation. We imagine \mathcal{S}_1 and a copy of \mathcal{S}_1 side by side. Both systems are initially in state 0. The transmitter uses an input in \mathcal{S}_1 that causes a transition into one of the states 1, 2, 3, or 4. The receiver then uses the input b in \mathcal{S}_1 . The state of \mathcal{S}_1 is now 5 or 6. The reader can see from figure 1 that the transmitter is forced to waste a move in both states 5 and 6 when the transmitter is on \mathcal{S}_1 . Thus it pays for the transmitter to temporarily switch over to the other copy of \mathcal{S}_1 when the first copy of \mathcal{S}_1 is in state 5 or 6. The transmitter now repeats the same steps for the copy of \mathcal{S}_1 as for \mathcal{S}_1 . Similarly, the receiver must waste a move in states 7 and 8 since the only possible output in response to its input is a 1; thus the receiver should temporarily switch to the other copy of \mathcal{S}_1 when the first copy of \mathcal{S}_1 is in state 7 or 8.

We now give the proof for (5). By Theorem 2.2, we have

$$V^n(\beta) = \max_{i \in I_R} \left\{ \sum_{o \in \mathcal{O}(\text{type}(\beta), i)} V^{n-1}(\beta io) \right\}$$

for all receiver output strings β . We claim that $i = b$ in the above equation. The following proposition will prove an equivalent statement.

Proposition 3.1 Let \mathcal{S}_1 be the controlled signalling system defined above. We then have

$$\sum_{o \in \mathcal{O}(\text{type}(\beta), b)} V^k(\beta bo) \geq V^k(\beta a 1) \quad (6)$$

for all integers $k \geq 0$.

Proof: We use induction on k for the proof. The proof of the $k = 0$ case is immediate since $V^0(\alpha) = 1$ for all receiver output strings α . Suppose the result holds for integers less than k .

Case a $\{7, 8\} \cap \text{type}(\beta) = \emptyset$

We notice that

$$\{si_1i_2 : i_1, i_2 \in I_T\} = \{si : i \in I_T\},$$

for states s of \mathcal{S}_1 , where $s \neq 7$ and $s \neq 8$. Also $sa = s$ for all states of \mathcal{S}_1 ; in other words, a is a receiver self-loop for all states s of \mathcal{S}_1 . We claim these two facts

imply $type(\beta b1) = type(\beta a1b1)$ if $1 \in \mathcal{O}(type(\beta), b)$, and $type(\beta b2) = type(\beta a1b2)$ if $2 \in \mathcal{O}(type(\beta), b)$. We will prove the first assertion; the proof of the second assertion follows similarly. We have

$$\begin{aligned} type(\beta a1) &= \{w : \text{there exists } x \in type(\beta), h_1 \in I_T \\ &\quad \text{such that } xh_1a = w \text{ and } out(xh_1, a) = 1, \} \\ &= \{w : \text{there exists } x \in type(\beta), h_1 \in I_T \\ &\quad \text{such that } xh_1 = w\}, \end{aligned} \quad (7)$$

where the first equality follows from Proposition 2.3. We also have

$$\begin{aligned} type(\beta a1b1) &= \{s : \text{there exists } w \in type(\beta a1), h \in I_T \\ &\quad \text{such that } whb = s \text{ and } out(wh, b) = 1\} \\ &= \{s : \text{there exists } x \in type(\beta), h, h_1 \in I_T, \\ &\quad \text{such that } xh_1hb = s \text{ and } out(xh_1h, b) = 1\} \\ &= \{s : \text{there exists } x \in type(\beta), h \in I_T, \\ &\quad \text{such that } xhb = s \text{ and } out(xh, b) = 1\} \\ &= type(\beta b1), \end{aligned} \quad (8)$$

where the first and last equalities follow from Proposition 2.3. The second equality (8) follows from substituting (7) into the first line; and the third equality follows from the two facts above. We now finish the proof of Case a. If we apply the definitions of V^{n+1} and Ext^{n+1} and use the fact that $|Ext^1(Q)| \geq |Q|$ for all nonempty sets $Q \subseteq Sig^m(a_0)$, we obtain $V^{n+1}(Q) \geq V^n(Q)$ for $n \geq 0$. Thus

$$\begin{aligned} \sum_{o \in \mathcal{O}(type(\beta), b)} V^k(\beta bo) &\geq \sum_{o \in \mathcal{O}(type(\beta), b)} V^{k-1}(\beta bo) \\ &= \sum_{o \in \mathcal{O}(type(\beta a1), b)} V^{k-1}(\beta a1bo) \\ &= V^k(\beta a1) \end{aligned}$$

where the last equality follows by the inductive hypothesis, and the previous equality follows by the results above and Theorem 2.2. We have proved Proposition 3.1 where $\{7, 8\} \cap type(\beta) = \emptyset$.

Case b $\{7, 8\} \cap type(\beta) \neq \emptyset$

We first show that

$$type(\beta a1b1) \subseteq type(\beta b1b1). \quad (9)$$

By applying Proposition 2.3 twice, we obtain

$$\begin{aligned} \text{type}(\beta b1b1) = \{s : \text{there exists } x \in \text{type}(\beta), h, h_1 \in I_T \\ \text{such that } xh_1bhb = s, \text{out}(xh_1, b) = 1, \\ \text{and } \text{out}(xh_1bh, b) = 1\}. \end{aligned} \quad (10)$$

The expression for $\text{type}(\beta a1b1)$ is given in (8) above; let $x \in \text{type}(\beta)$. If $x = 7$, then $\{0, 5, 6, 7\} \subseteq \text{type}(\beta a1b1)$, and $\{0, 5, 6, 7\} \subseteq \text{type}(\beta b1b1)$. The same holds if $x = 8$ with $\{0, 5, 6, 8\}$ in place of $\{0, 5, 6, 7\}$. Thus $x \in \text{type}(\beta a1b1)$ implies $x \in \text{type}(\beta b1b1)$ if $x \in \{7, 8\}$. Since $\text{type}(\beta) \cap \{7, 8\} \neq \emptyset$, the preceding argument shows that $\{0, 5, 6\} \subseteq \text{type}(\beta b1b1)$. Also, $\{1, 2, 3, 4\} \cap \text{type}(\beta a1b1) = \emptyset$. We have proved (9.)

We will now show that

$$\text{type}(\beta a1b2) \subseteq \text{type}(\beta b1b2) \cup \text{type}(\beta b2b1). \quad (11)$$

We apply Proposition 2.3 twice to obtain expressions for $\text{type}(\beta a1b2)$, $\text{type}(\beta b1b2)$, and $\text{type}(\beta b2b1)$ as in (10) above. The definition of \mathcal{S}_1 shows that $\text{type}(\beta a1b2) \subseteq \{5, 6, 8\}$. Since $\{7, 8\} \cap \text{type}(\beta) \neq \emptyset$, we have $\{5, 6\} \subseteq \text{type}(\beta b1b2)$. Suppose $8 \in \text{type}(\beta a1b2)$. Proposition 2.3 shows that $6 \in \text{type}(\beta)$; thus $8 \in \text{type}(\beta b2b1)$. The proof of (11) is complete.

To complete the proof of Case b, we need the following fact. Let $\alpha, \beta_1, \dots, \beta_m$ be receiver output strings such that $\text{type}(\alpha) \subseteq \bigcup_{i=1}^m \text{type}(\beta_i)$ where $m \geq 1$. We then have

$$V^n(\alpha) \leq \sum_{i=1}^m V^n(\beta_i) \quad (12)$$

for $n \geq 0$. We can prove (12) by induction. The inductive step is

$$\begin{aligned} V^k(\alpha) &= \max_{i \in I_R} \sum_{o \in \mathcal{O}(\text{type}(\alpha), i)} V^{k-1}(\alpha i o) \\ &= \sum_{o \in \mathcal{O}(\text{type}(\alpha), i')} V^{k-1}(\alpha i' o) \\ &\leq \sum_{o \in \mathcal{O}(\text{type}(\beta_j), i')} \sum_{j=1}^m V^{k-1}(\beta_j i' o) \\ &\leq \sum_{j=1}^m V^k(\beta_j) \end{aligned}$$

for some $i' \in I_R$. The first and last inequalities are due to Theorem 2.2. Hence

$$\sum_{o \in \mathcal{O}(\text{type}(\beta), b)} V^k(\beta b o) = \sum_{o \in \mathcal{O}(\text{type}(\beta), b)} \sum_{o' \in \mathcal{O}(\text{type}(\beta b o), b)} V^{k-1}(\beta b o b o') \quad (13)$$

$$\geq \sum_{o \in \mathcal{O}(\text{type}(\beta a 1), b)} V^{k-1}(\beta a 1 b o) \quad (14)$$

$$= V^k(\beta a 1) \quad (15)$$

where (13) and (15) follow from the inductive hypothesis and (14) follows from (9), (11), and (12) above.

The proof of Proposition 3.1 is complete. \square

We will now use Proposition 3.1 to show that $\text{cap}(\mathcal{S}_1) < 1$.

Proposition 3.2 If \mathcal{S}_1 is the controlled signalling system defined above, we have

$$\text{cap}(\mathcal{S}_1) < 1.$$

Proof: Let \mathcal{S}'_1 be the controlled signalling system obtained by removing a from $I_{1,R}$ in the controlled signalling system \mathcal{S}_1 . The *next* and *out* functions for \mathcal{S}'_1 are obtained by restricting the domain of next_1 and out_1 for \mathcal{S}_1 to $I_{1',R} = \{b\}$. Let $\beta = b o_1 \dots b o_m$, where $o_1, \dots, o_m \in \mathcal{O}_1$ and $m \geq 0$. Proposition 2.1 combined with Definitions 2.7, 2.9, and 2.10 shows that β is a receiver output string in \mathcal{S}_1 if and only if β is a receiver output string in \mathcal{S}'_1 . If β is a receiver output string and $n \geq 0$, we claim that

$$V^n(\mathcal{S}_1, \beta) = V^n(\mathcal{S}'_1, \beta). \quad (16)$$

(16) can be established by induction on n . For the inductive step, we apply Proposition 3.1 to obtain

$$V^n(\mathcal{S}_1, \beta) = \sum_{o \in \mathcal{O}(\text{type}(\beta), b)} V^{n-1}(\mathcal{S}_1, \beta b o). \quad (17)$$

We write $\text{type}(\mathcal{S}, \beta)$ in place of $\text{type}(\beta)$ in \mathcal{S} for a controlled signalling system \mathcal{S} . It is easy to check in Definitions 2.9 and 2.10 that $h_1 \dots h_m \in I_T^m$ is consistent with β and $a_0 h_1 i_1 \dots h_n i_n = a$ in \mathcal{S}_1 if and only if the same holds in \mathcal{S}'_1 . Thus $\text{type}(\mathcal{S}_1, \beta) = \text{type}(\mathcal{S}'_1, \beta)$ and $\mathcal{O}(\text{type}(\mathcal{S}_1, \beta), b) = \mathcal{O}(\text{type}(\mathcal{S}'_1, \beta), b)$. We can now apply the inductive hypothesis to (17) to prove (16).

If we apply (16) to the empty string, we get

$$V^n(\mathcal{S}_1, \epsilon) = V^n(\mathcal{S}'_1, \epsilon)$$

for $n \geq 0$. Since $\text{cap}(\mathcal{S}) = \text{rate}\{V^n(\mathcal{S}, \epsilon)\}$ for a controlled signalling system \mathcal{S} , it suffices to show $\text{cap}(\mathcal{S}'_1) < 1$. We will now compute the control array $\mu_{1'}$ of \mathcal{S}'_1 . The next definition will be helpful in this regard.

Definition 3.2 (Type tree) A type tree of a controlled signalling system \mathcal{S} is any rooted tree with labelled vertices having the following properties. The root has label (ϵ, a_0) where a_0 is the initial state of \mathcal{S} . In general, a vertex v of the tree is labelled with $(io : s_1, \dots, s_k)$ where $o \in O$ (O is the set of output symbols for \mathcal{S}), $i \in I_R$, and s_1, \dots, s_k are states of \mathcal{S} . The set $\{s_1, \dots, s_k\}$ is called the second part of the label, and io is called the first part of the label. Such a vertex v has $(i_1 o_1 : t_1, \dots, t_p)$ as the label of a child only if for each t_j , $1 \leq j \leq p$, there exists $h \in I_T$ and l , $1 \leq l \leq k$ such that $s_l h i_1 = t_j$ and $out(s_l h, i_l) = o_1$. For any type tree T for \mathcal{S} which has a vertex with $\{s_1, \dots, s_k\}$ as the second part of its label, there exists exactly one vertex with $\{s_1, \dots, s_k\}$ as the second part of its label that has children in T .

Let \mathcal{S} be a controlled signalling system with type tree T . Let $I_R = \{i_1, \dots, i_R\}$. Proposition 2.3 shows that every type τ of \mathcal{S} must occur as the second part of the label for some vertex v in T and that for every vertex v in T the second part of the label of v is a type of \mathcal{S} . Let v be the vertex in T that has children such that the second part of the label of v is s . The control array definition shows that $\mu(r, s, t)$ is the number of children w that v has in T where the second part of the label of w is t and the first part of the label of w is $i_r o$. If we apply these facts to \mathcal{S}'_1 , we obtain the control array of \mathcal{S}'_1 :

$$\mu_{1'}(b; s, t) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

By applying the definition of the \sim equivalence relation, we see that $\mu_{1'}(b; s, t)$ has 3 connected components, $\{1\}$, $\{2\}$, and $\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. The first two components are 1×1 zero entries; thus Proposition 2.4 gives that $cap(\mathcal{S}'_1) = d(\bar{\mu})$ where $\bar{\mu}$ is the matrix obtained from $\mu_{1'}(b; s, t)$ by eliminating the first two rows and columns. Let $\epsilon > 0$. By Theorem 2.3, $d(\bar{\mu}^\epsilon)$ is the \log of the largest positive eigenvalue of the matrix $\bar{\mu}^\epsilon$ which is obtained by adding ϵ to the zero elements of $\bar{\mu}$. Since the eigenvalues of a matrix depend continuously on the matrix entries (e.g. [2]), the largest positive eigenvalue of $\bar{\mu}^\epsilon$ approaches the largest positive eigenvalue α of $\bar{\mu}$ as ϵ goes to zero. By

Proposition 2.5, $d(\bar{\mu}^\epsilon)$ approaches $d(\bar{\mu})$ as ϵ goes to zero. The combination of these facts implies that $d(\bar{\mu}) = \log(\alpha)$. Since $\bar{\mu}$ is a connected component of the control array μ , $\bar{\mu}$ is an irreducible matrix. Thus nonnegative matrix theory (Chapter 2 of [3]) gives that α is less than 2 since the largest positive eigenvalue of an irreducible matrix is less than or equal to the largest row sum of the matrix with equality if and only if all row sums are equal. We have proved that $\text{cap}(\mathcal{S}_1) < 1$. \square

To complete the proof of (5), we will show that

$$\text{cap}(\mathcal{S}_1 \times \overline{\mathcal{S}_1}) \geq 1 \quad (18)$$

where $\overline{\mathcal{S}_1}$ is an isomorphic copy of \mathcal{S}_1 (we obtain $\overline{\mathcal{S}_1}$ by adding overlines to the input, output, and state sets of \mathcal{S}_1). By Theorem 2.1, it suffices to exhibit a block-policy code for $\mathcal{S}_1 \times \overline{\mathcal{S}_1}$ with a rate arbitrarily close to 1. We construct block-policy codes \mathcal{B}_n with rates $4n/(4n+1)$ where $n \geq 1$:

Definition 3.3 We define

$$\mathcal{B}_n = (a_0, 4n, 4n+1, X_n, \pi_n)$$

where

1. $a_0 = (0, \bar{0})$ is the initial state of $\mathcal{S}_1 \times \overline{\mathcal{S}_1}$.
2. $\pi_{4n+1} \in \Pi_{4n+1}$ is defined by

$$\pi_{4n+1}(i_1 o_1 \dots i_k o_k) = \begin{cases} \bar{b} & \text{if } k \bmod 4 \in \{2, 3\} \\ & \text{or } k = 4n \\ b & \text{otherwise.} \end{cases}$$

3. Let the transmitter input h in \mathcal{S}_1 where $\text{next}(7, h) = 0$ be denoted by w . We say that w causes the transmitter input transition $7 \rightarrow 0$. We may also assume that w causes transmitter input transitions $8 \rightarrow 0$, $0 \rightarrow 1$, $5 \rightarrow 5$, and $6 \rightarrow 6$. Let x cause transmitter input transition $0 \rightarrow 2$; we let y cause transmitter input transition $0 \rightarrow 3$. Let z cause transmitter input transition $0 \rightarrow 4$. We make the same definitions in $\overline{\mathcal{S}_1}$ by adding overlines to the above definitions. We define $h_1 \dots h_{4n+1} \in X_n$ if and only if for $1 \leq i \leq 4n+1$,

$$h_i = \begin{cases} \bar{w} & \text{if } i \bmod 4 = 1 \text{ and } i \neq 1, \\ & \text{or } i = 4n \\ w & \text{if } i \bmod 4 = 3 \\ w, x, y, \text{ or } z & \text{if } i \bmod 4 = 0 \text{ and } i \neq 4n, \\ & \text{or } i = 1 \\ \bar{w}, \bar{x}, \bar{y}, \text{ or } \bar{z} & \text{if } i \bmod 4 = 2. \end{cases}$$

It is easy to check that \mathcal{B}_n is a block-policy code with rate $4n/(4n+1)$ for $n \geq 1$. We have established (18); thus (5) follows from Proposition 3.2.

SECTION 4

R-CONTROLLED SIGNALLING SYSTEMS

In this section, we define a restricted-controlled signalling system, or r-controlled signalling system (r-css), establish the structure of the P-control array, and state and prove a product theorem. The r-controlled signalling systems are a subclass of the class of controlled signalling systems for which (4) holds. We will see that in the serial product of r-controlled signalling systems, the P-types play the same role as the types do in the analysis in Section 2. The P-types turn out to be Cartesian products of types of the individual systems in the product; we are therefore able to decompose the serial product of r-controlled signalling systems.

Definition 4.1 (r-css) An r-controlled signalling system is a controlled signalling system with the following additional two properties:

1. If there exists $h_1, h_2 \in I_T$ and states $s, t, u \in S$ such that $next(s, h_1) = t$ and $next(t, h_2) = u$, then there exists $h \in I_T$ such that $next(s, h) = u$.
2. For each $s \in S$, there exists $i_s \in I_T$ such that $next(s, i_s) = s$.

All the results from Section 2 must therefore hold for r-controlled signalling systems. We note that the product of r-controlled signalling systems is in general not a r-controlled signalling system.

Definition 4.2 (P-types) Let S_1 and S_2 be r-controlled signalling systems. Let $\beta = i_1 o_1 \dots i_n o_n$ be a receiver output string for the controlled signalling system $S_1 \times S_2$.

$$\begin{aligned}
 P\text{-type}(\beta) = \{ & a \in S : \text{there exists } h_1 h_2 \dots h_n \in I_T^n \\
 & \text{such that } h_1 h_2 \dots h_n \text{ is consistent with} \\
 & \beta, a_0 h_1 i_1 \dots h_n i_n = a, \text{ and } h_j \in I_{1T} \\
 & \text{if and only if } i_j \in I_{1R}, 1 \leq j \leq n \}.
 \end{aligned}$$

It is easy to construct examples such that $P\text{-type}(\beta) \neq \text{type}(\beta)$ where β is a receiver output string for the controlled signalling system $S_1 \times S_2$.

Lemma 4.1 Let $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$ be the product of the r -controlled signalling systems \mathcal{S}_1 and \mathcal{S}_2 , and let

$$\beta = i_1 o_1 \dots i_n o_n$$

be a receiver output string for \mathcal{S} . Let

$$\alpha = i_{r_1} o_{r_1} \dots i_{r_m} o_{r_m}$$

be the string obtained by deleting the symbols of I_{2T} and I_{2R} from β . Let

$$\gamma = i_{s_1} o_{s_1} \dots i_{s_l} o_{s_l}$$

be the string obtained by deleting the symbols of I_{1T} and I_{1R} from β . Then $\alpha \in \text{Sig}^m(a_{1_0})$ and $\gamma \in \text{Sig}^l(a_{2_0})$. Also

$$P\text{-type}(\beta) = \text{type}(\alpha) \times \text{type}(\gamma).$$

Conversely, if $\alpha \in \text{Sig}^m(a_{1_0})$ and $\gamma \in \text{Sig}^l(a_{2_0})$, then

$$\beta = \alpha \gamma$$

is a receiver output string for \mathcal{S} such that

$$P\text{-type}(\beta) = \text{type}(\alpha) \times \text{type}(\gamma).$$

Proof: We first show that the string α obtained by deleting the symbols of I_{2T} and I_{2R} from β satisfies $\alpha \in \text{Sig}^m(a_{1_0})$. There exists a strategy π for \mathcal{S} and $h_1 \dots h_n \in (I_{1T} \cup I_{2T})^n$ such that

$$\vdash_{(\pi, (a_{1_0}, a_{2_0}))} (h_1 \dots h_n) = (i_1 o_1 \dots i_n o_n).$$

For $1 \leq j \leq m$, we let

$$\text{ind}_{r_j} = \{v : r_{j-1} < v \leq r_j \text{ and } h_v \in I_{1T}\}$$

where we define $r_0 = 0$. Let h_{j_1}, \dots, h_{j_v} be an enumeration of the set ind_{r_j} where $j_1 < \dots < j_v$. Let

$$(e_j, f_j) = \text{endpt}(\pi, (a_{1_0}, a_{2_0}); h_1 \dots h_{r_j}),$$

$1 \leq j \leq m$, and let $e_0 = a_{1_0}$. Since \mathcal{S}_1 is an r -controlled signalling system, there exists $g_j \in I_{1T}$ such that

$$e_{j-1} g_j = e_{j-1} h_{j_1} \dots h_{j_v},$$

$1 \leq j \leq m$. If ind_{r_j} is empty, we let $g_j = i_{e_{j-1}}$ where $e_{j-1} i_{e_{j-1}} = e_{j-1}$, $1 \leq j \leq m$. Thus

$$\vdash_{(\pi, a_{1_0})} (g_1 \dots g_m) = i_{r_1} o_{r_1} \dots i_{r_m} o_{r_m}$$

where π_1 is a strategy for \mathcal{S}_1 such that

$$\pi_1(i_{r_1} o_{r_1} \dots i_{r_{t-1}} o_{r_{t-1}}) = i_{r_t},$$

$1 \leq t \leq m$. We have proved that α is a receiver output string for \mathcal{S}_1 . The same argument shows that γ is a receiver output string for \mathcal{S}_2 .

We now prove that

$$P\text{-type}(\beta) = \text{type}(\alpha) \times \text{type}(\gamma).$$

Let $(t_1, t_2) \in \text{type}(\alpha) \times \text{type}(\gamma)$. Thus the types definition gives that there exists $h_{r_1} h_{r_2} \dots h_{r_m} \in I_{1_T}^m$ such that $h_{r_1} h_{r_2} \dots h_{r_m}$ is consistent with α and

$$a_{1_0} h_{r_1} i_{r_1} \dots h_{r_m} i_{r_m} = t_1.$$

Also, there exists $h_{s_1} h_{s_2} \dots h_{s_l} \in I_{2_T}^l$ such that $h_{s_1} h_{s_2} \dots h_{s_l}$ is consistent with γ and

$$a_{2_0} h_{s_1} i_{s_1} \dots h_{s_l} i_{s_l} = t_2.$$

It is easy to check that $(t_1, t_2) \in P\text{-type}(\beta)$ since $h_1 \dots h_n$ is consistent with β ,

$$a_0 h_1 i_1 \dots h_n i_n = (t_1, t_2),$$

and $h_j \in I_{1_T}$ if and only if $i_j \in I_{1_R}$, $1 \leq j \leq n$.

Let $(t_1, t_2) \in P\text{-type}(\beta)$. Thus there exists $h_1 \dots h_n$ consistent with β such that $a_0 h_1 i_1 \dots h_n i_n = (t_1, t_2)$ and $h_j \in I_{1_T}$ if and only if $i_j \in I_{1_R}$, $1 \leq j \leq n$. It is easy to check (Definition 2.9) that $h_{r_1} \dots h_{r_m}$ is consistent with α and $a_0 h_{r_1} i_{r_1} \dots h_{r_m} i_{r_m} = t_1$. Hence $t_1 \in \text{type}(\alpha)$. The same argument shows that $t_2 \in \text{type}(\gamma)$.

We now prove the converse; let α and γ be receiver output strings for \mathcal{S}_1 and \mathcal{S}_2 , respectively. Thus there exist finite strategies π_1 and π_2 for \mathcal{S}_1 and \mathcal{S}_2 , respectively, and $h_1 \dots h_m \in I_{1_T}^m$ and $h_{m+1} \dots h_{m+l} \in I_{2_T}^l$ such that

$$\vdash_{(\pi_1, a_{1_0})} (h_1 \dots h_m) = \alpha$$

and

$$\vdash_{(\pi_2, a_{2_0})} (h_{m+1} \dots h_{m+l}) = \gamma.$$

Let

$$\pi_1 = \pi_1^1, \dots, \pi_m^1$$

and

$$\pi_2 = \pi_1^2, \dots, \pi_l^2$$

where $\pi_j^1 : (I_{1R} \times O)^{j-1} \rightarrow I_{1R}$ and $\pi_k^2 : (I_{2R} \times O)^{k-1} \rightarrow I_{2R}$, $1 \leq j \leq m$, $1 \leq k \leq l$. We then have

$$\pi_1, \pi_2 = \pi_1^1, \dots, \pi_m^1, \pi_1^2, \dots, \pi_l^2$$

where we define

$$\tilde{\pi}_j^2(x, y) = \pi_j^2(y), \quad 1 \leq j \leq l$$

for $x \in (I_R \times O)^m$ and $y \in (I_{2R} \times O)^{j-1}$. It then follows that

$$\vdash_{(\pi_1, \pi_2, (a_{10}, a_{20}))} (h_1 \dots h_{m+l}) = \alpha\gamma.$$

Thus $\beta = \alpha\gamma$ is a receiver output string for $\mathcal{S}_1 \times \mathcal{S}_2$. The first part of the lemma now shows that $P\text{-type}(\beta) = \text{type}(\alpha) \times \text{type}(\gamma)$. \square

Proposition 4.1 Let \mathcal{S}_1 and \mathcal{S}_2 be r -controlled signalling systems and let $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$. Let $h_1 \dots h_n$ be consistent with

$$\beta = i_1 o_1 \dots i_n o_n$$

such that

$$a_0 h_1 i_1 \dots h_n i_n = (s_1, s_2).$$

If $i_n \in I_{2R}$, (I_{1R}) , there exists $\tilde{h}_1 \dots \tilde{h}_n$ and $h \in I_{1T}$ (I_{2T}) such that $\tilde{h}_1 \dots \tilde{h}_n$ is consistent with β and

$$a_0 \tilde{h}_1 i_1 \dots \tilde{h}_n i_n h = (s_1, s_2)$$

where $\tilde{h}_j \in I_{1T}$ if and only if $i_j \in I_{1R}$, $1 \leq j \leq n$. Thus

$$\mathcal{O}(\text{type}(\beta), i) = \mathcal{O}(P\text{-type}(\beta), i).$$

Proof: To prove the first statement, we use induction on the length of β . We will prove the case where $i_n \in I_{2R}$; the proof of the other case is analogous.

Let $n = 1$. If $h_1 \in I_{2T}$, then we let $h = h_z$ where $z = \text{endpt}(a_0 h_1 i_1)$ and $z h_z = z$. We call h_z the self-loop at state z . Suppose $h_1 \in I_{1T}$. We let $h = h_1$ and $\tilde{h}_1 = h_z$ where $z = a_{20}$. (We recall that the initial state is (a_{10}, a_{20}) .) It then follows that \tilde{h}_1 is consistent with $\beta = i_1 o_1$ and $a_0 \tilde{h}_1 i_1 h = (s_1, s_2)$.

We assume the result holds for integers less than n . Let

$$\beta_1 = i_1 o_1 \dots i_{n-1} o_{n-1}.$$

It follows that $h_1 \dots h_{n-1}$ is consistent with β_1 ; let

$$(t_1, t_2) = a_0 h_1 i_1 \dots h_{n-1} i_{n-1}.$$

If $i_{n-1} \in I_{2R} (I_{1R})$, the induction hypothesis gives that there exists $\tilde{h}_1 \dots \tilde{h}_{n-1}$ and $g \in I_{1T} (I_{2T})$ such that $\tilde{h}_1 \dots \tilde{h}_{n-1}$ is consistent with β_1 and

$$a_0 \tilde{h}_1 i_1 \dots \tilde{h}_{n-1} i_{n-1} g = (t_1, t_2)$$

where $\tilde{h}_j \in I_{1T}$ if and only if $i_j \in I_{1R}$, $1 \leq j \leq n-1$. Let

$$(z_1, z_2) = \text{endpt}(a_0 \tilde{h}_1 i_1 \dots \tilde{h}_{n-1} i_{n-1}).$$

Case a $h_n \in I_{2T}$ and $i_{n-1} \in I_{2R}$. Thus $g \in I_{1T}$. We let $\tilde{h}_n = h_n$ and $h = g$. It is easy to check that $\text{out}(z_2 \tilde{h}_n, i_n) = o_n$ and $z_2 \tilde{h}_n i_n = s_2$. Since $\tilde{h}_n \in I_{2T}$, $i_n \in I_{2R}$, and $h \in I_{1T}$, it follows that $s_1 = t_1$. Thus the proof follows in this case.

Case b $h_n \in I_{2T}$, $i_{n-1} \in I_{1R}$. Thus $g \in I_{2T}$. We have $s_1 = t_1 = z_1$ and we let h be the transmitter self-loop for s_1 . Since S_2 is a r -controlled signalling system, we may choose \tilde{h}_n such that $z_2 g h_n = z_2 \tilde{h}_n$. We have $\text{out}(z_2 \tilde{h}_n, i_n) = o_n$ and $z_2 \tilde{h}_n i_n = s_2$. The proof of case b now follows.

Case c $h_n \in I_{1T}$, $i_{n-1} \in I_{2R}$. Thus $g \in I_{1T}$. We choose \tilde{h}_n to be the transmitter self-loop for state z_2 . We have $z_2 i_n = s_2$. Also, $\text{out}(z_2 \tilde{h}_n, i_n) = o_n$. We define h such that $z_1 g h_n = z_1 h$. Thus $z_1 h = s_1$ and the proof of case c follows.

Case d $h_n \in I_{1T}$, $i_{n-1} \in I_{1R}$. Thus $g \in I_{2T}$. Let $\tilde{h}_n = g$. We let $h = h_n$. We have $z_2 \tilde{h}_n = t_2$. Thus $\text{out}(z_2 \tilde{h}_n, i_n) = o_n$. Also, $z_1 h = s_1$. The proof of case d follows.

We now prove the second part of the proposition. We have

$$\mathcal{O}(P\text{-type}(\beta), i) \subseteq \mathcal{O}(\text{type}(\beta), i)$$

since $P\text{-type}(\beta) \subseteq \text{type}(\beta)$. For the other direction, let $o \in \mathcal{O}(\text{type}(\beta), i)$. Without loss of generality, we may assume $i \in I_{1R}$. There exists $(s_1, s_2) \in \text{type}(\beta)$ and $h \in I_{1T}$ such that $\text{out}((s_1, s_2)h, i) = o$. By the first part of the proposition, there exists $(t_1, t_2) \in P\text{-type}(\beta)$ and $\tilde{h} \in I_T$ such that $(t_1, t_2)\tilde{h} = (s_1, s_2)$.

Suppose $\tilde{h} \in I_{1T}$. We then have $t_1 \tilde{h} = s_1$ and $\text{out}(t_1 \tilde{h} h, i) = o$. There exists h_1 such that $\text{out}(t_1 h_1, i) = o$. Thus $o \in \mathcal{O}(P\text{-type}(\beta), i)$.

Suppose $\tilde{h} \in I_{2T}$. We then have $t_2 \tilde{h} = s_2$, and $t_1 = s_1$. Thus $o \in \mathcal{O}(P\text{-type}(\beta), i)$. \square

Proposition 4.2 (P-type growth properties) Let S_1 and S_2 be r -controlled signalling systems. Let β_1 and β_2 be receiver output strings for $S_1 \times S_2$ such that $P\text{-type}(\beta_1) = P\text{-type}(\beta_2)$. Let $i \in I_R$.

1. We have

$$\mathcal{O}(\text{type}(\beta_1), i) = \mathcal{O}(\text{type}(\beta_2), i).$$

2. Let $i \in I_{1R}$, and $o \in \mathcal{O}(\text{type}(\beta_1), i)$. If

$$P\text{-type}(\beta_1) = \text{type}(\alpha) \times \text{type}(\gamma)$$

then $o \in \mathcal{O}(\text{type}(\alpha), i)$ and

$$P\text{-type}(\beta_1 io) = \text{type}(\alpha io) \times \text{type}(\gamma).$$

An analogous statement holds if $i \in I_{2R}$.

3. Let $o \in \mathcal{O}(\text{type}(\beta_1), i)$. We have

$$P\text{-type}(\beta_1 io) = P\text{-type}(\beta_2 io).$$

Proof: The proof of the first statement follows immediately from the last statement of Proposition 4.1 and the fact that $P\text{-type}(\beta_1) = P\text{-type}(\beta_2)$. The proof of the second statement follows immediately from Lemma 4.1. The proof of the last statement follows immediately from the second statement. \square

Definition 4.3 (P-control array) Let \mathcal{S}_1 and \mathcal{S}_2 be r -controlled signalling systems and let $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$. Let w_1, \dots, w_l be an enumeration of the P-types of \mathcal{S} . Let i_1, \dots, i_R be an enumeration of the receiver input alphabet. We define the following array of integers to be the P-control array of \mathcal{S} :

$$\mu(r; w_i, w_j) = |\{o : \beta i, o \in \text{Sig}^{m+1}(a_0), \beta \text{ has length } m, \\ P\text{-type}(\beta) = w_i, \text{ and } P\text{-type}(\beta i, o) = w_j\}|$$

for $1 \leq i, j \leq l$ and $1 \leq r \leq R$.

Proposition 4.2 shows that the P-control array is well-defined.

Lemma 4.2 Let \mathcal{S}_1 and \mathcal{S}_2 be r -controlled signalling systems and let $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$. Let β_1 and β_2 be receiver output strings for \mathcal{S} . We also let $w_1 \dots w_l$ be an enumeration of the set of P-types of \mathcal{S} . We have:

1. For $n \geq 0$, $V^n(\beta_1) = V^n(\beta_2)$ if $P\text{-type}(\beta_1) = P\text{-type}(\beta_2)$. Thus the V^n 's are well-defined on the set of P-types.

2. Let w be a P-type. For $n \geq 1$,

$$V^n(w) = \max_r \sum_{j=1}^l \mu(r; w, w_j) V^{n-1}(w_j).$$

Proof: Theorem 2.2 gives that

$$V^n(\beta) = \max_r \sum_{o \in \mathcal{O}(\text{type}(\beta), i_r)} V^{n-1}(\beta i_r o) \quad (19)$$

for receiver output strings β and $n \geq 1$. We may now prove the first statement of the lemma by induction on n . The induction step follows by applying the first and last statements of Proposition 4.2 to (19). For the second statement of the lemma, we fix an output string β of P-type w . Since the number of terms on the right-hand side of (19) of a fixed P-type w_j is $\mu(r; w, w_j)$, the proof of the second statement follows from (19). \square

Let $I_R = \{i_1, \dots, i_R\}$ for a controlled signalling system S_1 . We define $C(r) = [\mu(r, s, t)]$, $1 \leq r \leq R$. We say that S_1 has control array $C(1), \dots, C(l)$.

Theorem 4.1 Let S_1 and S_2 be r -controlled signalling systems with control arrays $A(1), \dots, A(l)$ and $B(1), \dots, B(m)$, respectively. Let the types of S_1 and S_2 be s_1, \dots, s_p and t_1, \dots, t_q , respectively. We choose

$$s_1 \times t_1, \dots, s_p \times t_1, \dots, s_1 \times t_q, \dots, s_p \times t_q$$

as our ordering for the P-types of $S = S_1 \times S_2$. Then $S_1 \times S_2$ has P-control array

$$\mu(1, s, t), \dots, \mu(l + m, s, t)$$

where

$$\mu(r, s, t) = \begin{bmatrix} A(r) & 0 & \dots & 0 \\ 0 & A(r) & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & A(r) \end{bmatrix} \quad 1 \leq r \leq l,$$

$$\mu(r, s, t) = \begin{bmatrix} B(u)_{11}I_p & B(u)_{12}I_p & \dots & B(u)_{1q}I_p \\ B(u)_{21}I_p & B(u)_{22}I_p & \dots & B(u)_{2q}I_p \\ \vdots & \vdots & & \vdots \\ B(u)_{q1}I_p & B(u)_{q2}I_p & \dots & B(u)_{qq}I_p \end{bmatrix},$$

$$u = r - l, \quad l + 1 \leq r \leq l + m,$$

and I_p is the $p \times p$ identity matrix.

Proof: The proof follows from our ordering of the P-types combined with the second statement of Proposition 4.2. \square

We are now in a position to prove formula (4) for r-controlled signalling systems.

Theorem 4.2

$$\text{cap}(\mathcal{S}_1 \times \mathcal{S}_2) = \max\{\text{cap}(\mathcal{S}_1), \text{cap}(\mathcal{S}_2)\}$$

where \mathcal{S}_1 and \mathcal{S}_2 are r-controlled signalling systems.

Proof: Let $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$. We use induction on n to prove the following formula:

$$V^n(\mathcal{S}; s \times t) \leq \sum_{k=0}^n V^k(\mathcal{S}_1; s) V^{n-k}(\mathcal{S}_2; t) \quad (20)$$

where s and t are types for \mathcal{S}_1 and \mathcal{S}_2 , respectively. The $n = 1$ case is straightforward and is left to the reader. Suppose (20) is true for $n - 1$.

$$V^n(\mathcal{S}, s \times t) = \max_r \sum_w \mu(r, s \times t, w) V^{n-1}(\mathcal{S}, w) \quad (21)$$

$$= \sum_w \mu(\hat{r}, s \times t, w) V^{n-1}(\mathcal{S}, w) \quad (22)$$

$$= \sum_{w_1} \mu(\hat{r}, s \times t, w_1 \times t) V^{n-1}(\mathcal{S}, w_1 \times t) \quad (23)$$

$$\leq \sum_{w_1} \mu_1(\hat{r}, s, w_1) \sum_{k=0}^{n-1} V^k(\mathcal{S}_1; w_1) V^{n-1-k}(\mathcal{S}_2; t) \quad (24)$$

$$= \sum_{k=0}^{n-1} V^{n-1-k}(\mathcal{S}_2; t) \sum_{w_1} \mu_1(\hat{r}, s, w_1) V^k(\mathcal{S}_1; w_1)$$

$$= \sum_{k=0}^{n-1} V^{n-1-k}(\mathcal{S}_2; t) V^{k+1}(\mathcal{S}_1, s) \quad (25)$$

$$\leq \sum_{k=0}^n V^{n-k}(\mathcal{S}_2; t) V^k(\mathcal{S}_1, s).$$

Equation (21) is the second statement of Lemma 4.2. In (22), \hat{r} is the maximum r value from (21); we have assumed that $i_{\hat{r}} \in I_{1R}$. The argument is the same in the case where $i_{\hat{r}} \in I_{2R}$. Equation (23) follows from the structure of the P-control array. Inequality (24) is the inductive hypothesis combined with the fact that $\mu(\hat{r}, s \times t, w_1 \times t) = \mu_1(\hat{r}, s, w_1)$ where μ_1 is the control array for \mathcal{S}_1 . Equation (25) follows from applying Theorem 2.2 (the optimality equation). Thus we have completed the induction proof for (20).

Theorem 2.1 gives that

$$\text{cap}(\mathcal{S}_1) = \limsup_{n \rightarrow \infty} \frac{\log d^n(\mathcal{S}_1, a_0)}{n} \quad (26)$$

where \mathcal{S}_1 is a controlled signalling system. Let $c_1 = \text{cap}(\mathcal{S}_1)$ and $c_2 = \text{cap}(\mathcal{S}_2)$. We choose $c > \max\{c_1, c_2\}$. By (26), we can choose $L \geq 1$ such that $V^l(\mathcal{S}_1, a_{1_0}) \leq 2^{lc}$ and $V^l(\mathcal{S}_2, a_{2_0}) \leq 2^{lc}$ for $l \geq L$. We recall from section 2

$$\text{rate}\{x_n\} = \limsup_{n \rightarrow \infty} \frac{\log x_n}{n} \quad (27)$$

for any infinite sequence $\{x_n\}$. We choose $M \geq 1$ such that

$$\max\{V^L(\mathcal{S}_1; a_{1_0}), V^L(\mathcal{S}_2; a_{2_0})\} \leq M.$$

We now have

$$\begin{aligned} V^n(\mathcal{S}; a_{1_0} \times a_{2_0}) &\leq \sum_{k=0}^n V^k(\mathcal{S}_1; a_{1_0}) V^{n-k}(\mathcal{S}_2; a_{2_0}) \\ &= \sum_{k=0}^L V^k(\mathcal{S}_1; a_{1_0}) V^{n-k}(\mathcal{S}_2; a_{2_0}) + \sum_{k=n-L}^n V^k(\mathcal{S}_1; a_{1_0}) V^{n-k}(\mathcal{S}_2; a_{2_0}) + \\ &\quad \sum_{k=L+1}^{n-L-1} V^k(\mathcal{S}_1; a_{1_0}) V^{n-k}(\mathcal{S}_2; a_{2_0}) \\ &\leq M(L+1)V^n(\mathcal{S}_2; a_{2_0}) + M(L+1)V^n(\mathcal{S}_1; a_{1_0}) + \\ &\quad \sum_{k=L+1}^{n-L-1} 2^{kc} 2^{(n-k)c} \\ &\leq M(L+1)V^n(\mathcal{S}_1; a_{1_0}) + M(L+1)V^n(\mathcal{S}_2; a_{2_0}) + (n-2L-1)2^{nc}. \end{aligned}$$

If $\{x_n\}$ and $\{y_n\}$ are infinite sequences, it easy to show that

$$\text{rate}\{x_n + y_n\} = \max\{\text{rate}\{x_n\}, \text{rate}\{y_n\}\}. \quad (28)$$

Equation (28) applied to the last member of the previous chain of inequalities gives

$$\begin{aligned} \text{rate}\{V^n(\mathcal{S}; a_{1_0} \times a_{2_0})\} &\leq \max\{c_1, c_2, c\} \\ &= c. \end{aligned} \quad (29)$$

Equations (26) and (27) applied to the left side of (29) give that

$$\text{cap}(\mathcal{S}) \leq c.$$

The proof now follows. \square

The definitions and results of this section can be extended to products of n r- controlled signalling systems.

LIST OF REFERENCES

1. Bellman, R., 1955, "On a Quasi-Linear Equation," In *Canadian Journal of Mathematics*.
2. Franklin, J., 1968, *Matrix Theory*, Prentice Hall, Englewood Cliffs, NJ.
3. Minc, H., 1988, *Nonnegative Matrices*, John Wiley and Sons, Inc., New York, NY.
4. Shannon, C. E. and Weaver, W., 1949, *The Mathematical Theory of Communication*, University of Illinois Press.
5. Wittbold, J. T., 1989, "Controlled Signalling Systems and Covert Channels," In *Proceedings of the Computer Security Foundations Workshop II*, Franconia, NH.

DISTRIBUTION LIST

INTERNAL

D70

E. H. Bensley

D82

D. J. Muder

G110

H. A. Bayard
E. L. Lafferty
L. J. LaPadula
J. K. Millen
P. S. Tasker

G116

F. Belvin
W. R. Gerhart
M. A. Mercier (3)

G117

D. J. Bodeau
T. J. Brando
P. W. Brown
R. K. Burns
F. N. Chase
C. M. Chiles
M. Daya
W. M. Farmer
D. H. Friedman
H. G. Goldman
R. P. Goldsmith

G117 (concluded)

J. E. Grenier
J. D. Guttman
C. D. Hunter
L. P. Immes
J. V. A. Janeri
D. M. Johnson
M. S. Kannel
F. L. Knowles
H. P. Ko
R. C. Labonté
J. I. Leivent
M. B. Michnikov
J. K. Millen
L. G. Monk
M. E. Nadel
R. L. Parker
M. J. Prella
J. D. Ramsdell
H. H. Rubinovitz
B. G. Shenouda
I. G. Smotroff
V. Swarup
J. F. Thayer
B. M. Thuraisingham
J. T. Trostle (5)
M. L. Urban
R. J. Watro
J. G. Williams
J. T. Wittbold
A. M. Wollrath
M. M. Zuk

EXTERNAL

National Security Agency
9800 Savage Road (AS11)
Fort George G. Meade, MD 20755-6000

Terry Ireland, R2
Robin Jule, R231
Bob Morris
Sami Saydjari, R231
Brian Snow, R2
Howard Stainer, R23 (5)